PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-041051
(43)Date of publication of application : 09.02.1990

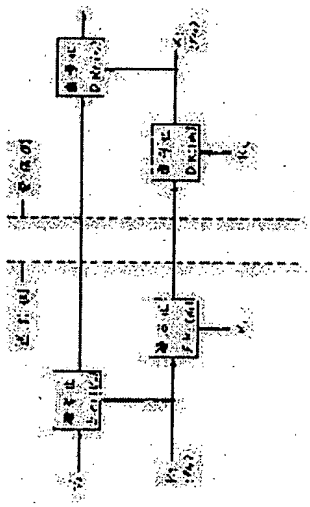
(51)Int.Cl. H04L 9/06
H04H 1/00
H04L 9/14
H04N 7/167

(21)Application number : 63-191781
(22)Date of filing : 29.07.1988

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
KONDEISHIYONARU AKUSESU TECHNOL KENKYUSHO:KK
(72)Inventor : HIRASHIMA MASAYOSHI
SATO TOSHICHIKA

(54) RECORDING SYSTEM

(57)Abstract:
PURPOSE: To attain the decoding of recording information for a specific cryptographic decoder only by ciphering a key Kt to decode cryptographic information by a key Ki specific to each decoder so as to form a key EKi (Kt) and recording it together with cryptographic information.
CONSTITUTION: Suppose that a video signal and a voice signal are scrambled by using a function f(Kt) decided definitely with a key Kt changing as time elapses, then in the case of sending the key Kt from the sender side to the receiver side, since the possibility of interception exists without any modification, the key is ciphered by other key Ki to form a key EKi and it is recorded on a VTR or the like together with cryptographic information. When the recorded information is reproduced, since the key EKi (Kt) is obtained, the result DKi (Kt) being the decoding of the EKi (Kt) is decoded by using further the key Ki to obtain the key Kt, and then the reproduced scrambling information signal is decoded.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−41051

⑤Int. Cl.⁵	識別記号	庁内整理番号	㊸公開　平成2年(1990)2月9日
H 04 L 9/06			
H 04 H 1/00	F	7608−5K	
H 04 L 9/14		8725−5C	
H 04 N 7/167		7240−5K	
	H 04 L 9/02		Z

審査請求　未請求　請求項の数 7　(全8頁)

㊹発明の名称　記録システム

㉑特　願　昭63−191781
㉒出　願　昭63(1988)7月29日

㉒発明者　平嶋　正芳　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉒発明者　佐藤　寿親　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉑出願人　株式会社コンディショナル・アクセス・テクノロジー研究所　東京都港区虎ノ門1丁目19番地10号
㉔代理人　弁理士　粟野　重孝　外1名

明　細　書

1、発明の名称

記録システム

2、特許請求の範囲

(1) 階層構造をとる複数の鍵により記録データを暗号化及び復号化する記録システムであって、暗号化した映像信号と一定の時間を経過した時に更新される鍵K_tを含む制御信号とを同一の記録媒体上に記録するに際し、上記鍵K_tをシステム中の暗号解読装置に固有な鍵K_iを用いて暗号化した$E_{K_i}(K_t)$として記録するようにしたことを特徴とする記録システム。

(2) 鍵K_tより更新周期の長い鍵K_xを鍵K_tと共に用いるようにし、鍵K_tを鍵K_xで暗号化し、鍵K_xを鍵K_iで暗号化して、$E_{K_i}(K_x)$の形で記録するようにしたことを特徴とする請求項1記載の記録システム。

(3) 信号送出側から送られてくる鍵K_tの送出形式と同一の形式で、暗号解読装置から$E_{K_i}(K_t)$を解読した$D_{K_i}(K_t)=K_t$を出力し、同時に映像信号と音声信号を再生して出力するようにしたことを特徴とする請求項1記載の記録システム。

(4) 信号送出側から送られてくる鍵K_xの送出形式と同一の形式で、暗号解読装置から$E_{K_i}(K_x)$を解読した$D_{K_i}(K_x)=K_x$を出力し、同時に映像信号と音声信号を再生して出力するようにしたことを特徴とする請求項2記載の記録システム。

(5) 記録される信号が鍵K_tにより暗号化されていることを特徴とする請求項1、または3記載の記録システム。

(6) 記録される信号が鍵K_tにより暗号化されていることを特徴とする請求項2または4項記載の記録システム。

(7) 有料視聴デコーダ内において、記録された信号を再生して得られる復号化用の制御信号の処理回路と、放送局から送られて来る信号中の復号化用の制御信号の処理回路とを部分的に共通にするとともに、両回路の切替えを外部から行うことを物理的に阻止する構造にしたことを特徴とする請求項1～5のいずれかに記載の記録システム。

3、発明の詳細な説明

産業上の利用分野

本発明は、情報を暗号化して記録し、特定の再生装置によってのみ再生できるようにする記録システムに関する。

従来の技術

情報（映像・音声・データ）を暗号化して伝送・受信することは従来から知られているが、暗号化する場合、秘密を保ちたい情報と、料金を支払った者にだけ見せる情報とがある。秘密を保ちたい場合は情報を暗号化したままの状態で記録するようにすればよいが、その場合にはどの暗号復号装置ででも解読できるというのでは望ましくない。また、有料の場合は、解読された情報がコピーされること望ましくない。

本発明は、これらの課題を解決する記録システムに関する技術である。

発明が解決しようとする課題

従来の記録システムにおいては、暗号化したまま記録する場合であっても、どの復号装置ででも解読できるという問題があった。

また、暗号化された情報を解読して記録する場合は例えば機器の密番を符号化して同時に記録していたが、解読された情報のコピーを防ぐことができないという問題があった。

そこで、本発明はかかる従来の問題を解消して、特定の暗号復号器でのみ記録情報を解読することができ、また、解読された情報のコピーを防止することもできる記録システムを提供することを目的とする。

課題を解決するための手段

この目的を達成するため、本発明においては、暗号化情報を解読するための鍵K_t又はK_xを各々の解読装置に固有の鍵K_iで暗号化して$E_{K_i}(K_x)$とし、暗号化情報とともに記録するようにした点に特徴がある。従って、記録された情報をそのまま再生しても暗号化されたままであり、記録に用いられた鍵K_iを有する暗号解読装置によってのみ解読できる。

作　用

このような本発明によると、一般には鍵K_t又はK_xは時間が経過すると変化するので、再生時に暗号解読装置の鍵K_t又はK_xが情報信号を記録した時とは異なっていると、再生した時にスクランブル化された映像や音声等の暗号化情報が復元できないが、本発明の記録システムによれば、記録した情報信号を再生したときに$E_{K_i}(K_t)$又は$E_{K_i}(K_x)$が得られるので、これを解読した$D_{K_i}(K_t)$又は$D_{K_i}(K_x)$をさらに鍵K_iで解読することによりK_xを得て、再生したスクランブル化情報信号を解読（デスクランブル化）することができる。

実　施　例

本発明の一実施例を第１図に示す。図中、１～５の部分は記録再生部（たとえばＶＴＲ）であり、１１～２１，２９の部分は暗号解読機能及び暗号化機能を含む有料デコーダの一部を示す。

第１図中、入力バッファ回路１．３、映像記録ヘッド４、音声記録ヘッド５は通常のＶＴＲの該当部分と共通の回路等である。また、データ抜取回路１４、暗号復号化回路１５、鍵K_tメモリ16は、既に実用化されている有料放送（例えばVideo Cipher ⅡやＢＭＡＣ等）の有料デコーダの当該部分と機能的に同一の回路である。

まず、本発明の記録システムの基礎となる暗号化システム全体の概要を第２図，第３図を参照して説明する。ここでは、時間の経過により変化する鍵K_tによって一義的に決まる関数$f(K_t)$により映像信号及び音声信号をスクランブル化するものとする。鍵K_tを送出側から受信側へ伝送する場合。そのままの形では盗聴されるおそれがあるので、別の鍵K_iで暗号化する。鍵K_iは、端末１台ずつに別々のものを割当てても、数台まとめて一の鍵を割当ても、全端末に共通の鍵を使用してもよい。このような鍵の重層構造については、たとえば、一松信監修「データ保護と暗号化の研究」第６３頁図１－２７、等に記載されている。鍵K_tとK_iの間に、もう一つ鍵K_tより長い周期で更新される鍵K_xを用いてもよい。このことも同文献に示されている。第３図がその例である。

ここでは、説明を簡単にするために、第２図の

場合について説明する。放送の形式として、鍵等の制御信号をデジタル信号で送出できる放送衛星ＢＳ２で採用されている方式を考える。この方式は、音声をデジタル信号で伝送するので、その音声データにＰＮ信号を加算すれば暗号化（スクランブル化）できる。従って、そのＰＮ信号の初期値がすなわち鍵K_tとなり、これが判れば復号化（デスクランブル化）できる。この鍵K_tを鍵K_iで暗号化（スクランブル化）して送り、受信側で鍵K_iで復号化すればよい。映像信号については、ラインローテーションによる暗号化（スクランブル化）を行ない、その各ラインでの切断点を上記ＰＮ信号で与えればよく、これについては公知の技術が使える。

さて、第１図において、P_1は受信側での受信信号の入力端子で、例えばＢＳチューナのＦＭ検波複合映像出力信号をそのまま入力すればよい。11は入力バッファ回路、１２は5.73MHzの音声搬送波成分と映像信号成分とを分離する分離回路、１３は5.73MHzのＱＰＳＫ信号を復調し2.048Mbpsのデジタル信号を得る復調回路である。14はＱＰＳＫ復調回路１３の出力から音声データ以外の制御信号データを抜取りる抜取回路、１５はその制御信号データから暗号化されている鍵K_tその他の信号を復号する復号化回路、１６は復号化回路１５の出力中の鍵K_tを記憶するメモリＡである。なお、メモリＡ１６の他に鍵K_t以外の制御信号を記憶するメモリが別にあることはいうまでもない。

一方、１７は4.5MHzの連続搬送波を2.048Mbpsの音声データで振幅変調する変調回路であり、変調回路１７の変調音声出力と分離回路１２の映像信号成分出力とを混合回路１８で混合し、出力端子P_2より出力する。従って、出力端子P_2の出力信号は地上テレビ放送のＮＴＳＣ方式のテレビ信号と類似のものとなり、ＡＭ変調された4.5MHzの音声データ信号が含まれていることになる。

この信号がＶＴＲの入力バッファ回路１を介して映像記録ヘッド４でテープに記録される。この場合、映像記録ヘッド４は4.5MHz以上の高域まで記録可能であることはいうまでもない。なお、ＶＴＲの記録帯域が狭い場合には音声データ信号をベースバンドで記録すればよいが、ベースバンドの音声データ信号をスクランブル化して記録するためには、有料デコーダ側に音声スクランブル化回路が必要になる。このことは、本発明の主題ではないので、ここでは、ＶＴＲで4.5MHzまで記録できるものとしておく。

一方、メモリ１６に記憶された鍵K_tは暗号化回路１９でメモリ２９からの端末固有の鍵K_i（ここでは、１端毎に鍵K_iが異なるものとする）で暗号化し、出力バッファ回路２０を介して出力端子P_3より出力する。暗号化回路１９及び出力バッファ回路２０はそれぞれの内部にバッファメモリを有するものである。

今、第４図に示す時刻t_0にＶＴＲの記録開始制御回路２で記録開始を指示すると、ϕ_0の制御信号が、１，３，４，５の各回路へ伝えられ、有料デコーダの出力端子P_2，P_3からの出力信号を同一のテープに記録する。次に、有料デコーダ側で時刻t_1に切換スイッチ２２を操作すると、Ｒ／Ｗ制御回路２１から制御信号ϕ_1（ϕ_{11}），ϕ_2（ϕ_{12}）が出力され、メモリ１６から鍵K_tを読み出して暗号化回路１９へ入力し、暗号化回路１９で鍵K_iにより暗号化して$EK_i(K_t)$として出力バッファ回路２０へ伝え、そのバッファメモリへ書込む。この作用がt_1～t_2の間に終り、続いてt_2～t_3の間に出力バッファ回路２０から1200bpsの低速でその$EK_i(K_t)$を読み出し、出力端子P_3から出力する。その信号の形式をデータ抜取回路１４で抜取った出力と同じパケット構造とし、１パケットを２７２ビットとする。ここでは出力バッファ回路２０から$EK_i(K_t)$を1200bpsでフェイズエンコードして読み出すものとすれば、約0.23秒で２７２ビットのデータを出力することができる。これをＶＴＲの入力バッファ回路３を介して音声記録ヘッドで音声トラックに記録する。ＶＴＲの音声トラックの記録帯域は、5KHz以上あり、1200bpsで読出されるデータをフェイズエンコードして得られる出力信号の最高周波数成分より十分高域まで伸びているので、記録上の問題はな

い。このようにしてＶＴＲのテープの音声トラックに$E_{K_i}(K_t)$を記録する場合、最初に１回だけϕ_2の如く$t_2 \sim t_3$の間のみに記録する場合と、ϕ_{12}の如く一定間隔で$t_{n2} \sim t_{n3}$の間にくり返し記録する方法があるが、どちらでもよい。その記録制御用の信号ϕ_1又はϕ_{11}はＲ／Ｗ制御回路21で形成し、切換スイッチ２２の設定により切換える。

以上の如く構成すれば、第４図の記録制御信号ϕ_0が高レベルの間に暗号化されている映像信号(音声コード信号を含む）をＶＴＲに映像記録ヘッド４により記録し、かつ鍵K_tも暗号化して$E_{K_i}(K_t)$としてＶＴＲの音声トラックに音声記録ヘッド６により記録することができる。この場合、記録再生部のＶＴＲとして既存のＶＴＲを使うことができる。なお、ＶＴＲにおける映像信号の記録帯域幅が広ければ変調回路１７を用いずに入力バッファ回路１１の出力を直接出力端子P_2へ出力し、そのまま映像記録ヘッド４へ伝えて記録することも可能である。

次に、このようにして記録された映像・音声信号と鍵との再生について、第５図を参照して説明する。第４図で説明したように、再生信号の始めの部分の$t_2 \sim t_3$のみに$E_{K_i}(K_t)$が記録されている場合と、$t_{n2} \sim t_{n3}$にくり返して記録されている場合があるが、どちらでも同じように動作する。先ず、記録再生部の再生開始制御回路１０で再生開始を制御すると、音声再生ヘッド７で音声トラックから暗号化した$E_{K_i}(K_t)$のフェイズエンコード信号を再生し、出力バッファ回路９を介して有料デコーダの入力端子P_5に入力する。入力バッファ回路２７でその出力信号をフェイズデコードして1200bpsの２７２ビットのデジタル信号$E_{K_i}(K_t)$に戻す。その入力バッファ回路２７の出力$E_{K_i}(K_t)$をメモリ２９に記憶されている端末固有の鍵K_iで復号化（デコード）して鍵K_tを得る。この鍵K_tをK_tメモリＢ３０に書込む。

一方、このときＶＴＲ再生指示回路３１から再生指示信号を発してK_tメモリＡ１６、セレクタ26、K_tメモリＢ３０、デスクランブル処理部３２へ供給する。これにより、K_tメモリＡ１６はその出力がハイインピーダンスとなり、保持状態となり、他方のK_tメモリＢ３０が能動状態になる。また、このときセレクタ２６はＱＰＳＫ復調回路１３の出力に代えて音声検波回路２５の出力をデータ処理回路１４へ加える。従って、データ処理回路１４にはＱＰＳＫ復調回路１３の出力と同形式の音声検波回路２５の出力が加える。このデータ処理回路１４は、ＱＰＳＫ復調回路１３の出力も音声検波回路２５の出力も同じように処理する。そして、暗号復号回路１５でデータ中の一部の制御信号の暗号を解読する。この１５の動作については後述する。暗号復号回路１５の出力中の鍵K_t以外の情報はデスクランブル処理部３２へ伝える。

デスクランブル処理部３２では鍵K_tを用いてデータ抜取回路１４の出力の一部（暗号復号回路15で解読していない部分）の解読を行ない、復号化（デスクランブル）について必要な情報を得、その情報に基づき再生信号をデスクランブルする。音声データ信号の復号化（デスクランブル）は音声データのフレーム周期の初めに所定のＰＮ初期値即ち鍵K_tを与えてＰＮ系列を発生させ、そのＰＮ値をデータ処理部１４の出力の音声データ信号に加算することによって行なう。

映像信号については、その暗号化の際にラインローテーションのカット位置をＰＮ値で指定し、例えば第２２ライン目のカット位置を鍵K_t即ちＰＮの初期値で指定し、以下、第２３，２４……２６２ライン目までＰＮ系列の示す位置で１ラインの映像信号をカットしローテーションする。このとき、毎フィールド又は毎フレームでの同じラインは同じ位置でカットする。ラインローテーション前のあるライン映像信号の波形が第８図Ａに示すようなものであったとすれば、所定のＰＮ値で示される位置でカットしてローテーションすることにより暗号化した波形は第８図Ｂのようなものとなる。従って、その鍵K_tにより初期のＰＮ値が決定できれば、第８図Ｂの暗号化映像信号を復号してＡへ戻すことは容易である。

ここで、復号化（デスクランブル）に用いる鍵

K_tが1週間単位で変更されるものとすると、上述したような受信及び記録に用いた有料デコーダを用いてＶＴＲから再生しても、一週間後にはその鍵K_tが変更されていて第５図中のK_tメモリＡ１６の鍵K_tは記録時のものとは異なっている。従って、このような場合にはＶＴＲの再生信号からK_tを得る必要がある。又、上述のように、記録時に鍵K_tを鍵K_iを用いて暗号化しているので、録画時に用いた有料デコーダ以外の有料デコーダを用いてもその鍵K_iを有していないためにもはや鍵K_tが得られないことになり、再生信号のスクランブルを解くことはできない。

なお、鍵K_tが変化していないことが判っているときには、第５図の構成において再生時にK_tメモリＢ３０の出力を用いずに、K_tメモリＡ１６の出力を用いてデスクランブル処理部３２で再生信号をデスクランブルするように改造することにより、鍵K_tが次に変更されるまでは再生信号から復号化したK_tを用いなくても、すなわちK_iを用いなくても再生信号をデスクランブルすることが可能になってしまう。つまり、固有の鍵K_iを有していない有料デコーダでも、伝送信号からK_tを取り出すことができるものであれば、鍵K_iで暗号化して記録した信号を再生することができる。つまり、実質的な盗視聴が可能になる。このようなことを防ぐには、鍵K_tを比較的短期間で変化更すること、及び、第５図の有料デコーダにおいてＶＴＲ再生指示がされたときにK_tメモリＡ１６から読み出した鍵K_tによってデスクランブルすることが簡単にできないように、この切換部を改造できない構造にすることにより、同一の有料デコーダによる個人的な記録再生以外をできなくすることができ、不法な複製テープの作成を阻止できる。第９図はそのような構成の一例を示す。ＶＴＲ再生指示回路３１をスイッチ３１Ｓとその入力を保持するメモリ３１Ｍとにより構成し、このメモリ３１Ｍと鍵K_tメモリＡ１６、鍵K_tメモリＢ３０及びセレクタ30を一体化して１つのパッケージに封入するか樹脂モールドすることにより、ＶＴＲ再生時に受信信助から取り出した鍵K_tを使用するような切換えを物理的に阻止して改造を防止できる。

次に、上述したような鍵K_tの暗号化（スクランブル化）の具体的な内容と、暗号復号化回路１５の動作について、第６，７図を用いて補足説明する。ここでは、鍵K_tの更新周期を毎週１回とし、夜間に行なうものとする。なお、有料デコーダ端末の電源が切断されていると有料デコーダ内のK_tメモリＡ１６のK_tを更新できないので、念のために毎日深夜に鍵K_tを鍵K_iで暗号化して各端末の有料デコーダへ送るものとする。仮に、音声データ信号のＱＰＳＫ変調信号を用いて各種データを送るものとし、その毎秒2.048Mビット中の500Ｋビットを鍵K_tの配送に使うものとする。また、１端末当りの鍵K_tを３２ビットとし、アドレスを２４ビットとすると、１端末当り５６ビット必要である（第７図参照）。また、伝送する１パケットを、ヘッダを含めて第６図の如く２８８ビットとする。Ａは識別信号１が付された各種制御情報用のパケット、Ｂは認別信号２が付されK_tを含む制御信号用のパケットである。２７２ビットを文字放送に使われているＢＥＳＴ方式による誤り訂正方式の符号化によって構成すれば、データは２７２ビット中の１９０ビットとなる。従って、一端末当り５６ビットとすると３端末分の１６８ビットのデータを１パケットで伝送することができる。５００Ｋビット÷２８８ビット≒1736が毎秒アクセスできる端末数であり、アドレスを２４ビットで構成すると指定可能数は約1678万端末であるから、16,780,000÷1736≒0.966万秒即ち約2.7時間で全端末をアクセスして鍵K_tを配送することができる。そこで、例えば月曜日の早朝２時～５時に１回鍵K_tを配送し、後は端末側からの要求に応じてその都度個別対応する等の方法が選べる。

第６図Ｂの信号形式（パケット）のＱＰＳＫ変調によるデーを受信した場合、暗号復号信号１５ではその識別信号が(2)であることを識別して鍵K_tが送られてきていることを識別し、これを自己の有する鍵K_iで解読し、端末アドレスと一致する暗号化された鍵K_tをもう一度鍵K_iで解読する。即ち、

鍵K_tが二重に暗号化されているので、二重に復号化する。鍵K_tのみ暗号化してアドレスは暗号化しない方法、鍵K_tを他のK_i'で暗号化しておく方法もある（K_i'は端末毎に異なるK_i以外の鍵である）。

一方、第６図Ａの信号形式の信号を受信した場合は、暗号化回路１５で鍵K_tを用いて制御情報を解読し、復号化（デスクランブル化）に必要な情報を得る。

以上は鍵の構造が第２図の如く二重の場合であるが、第３図の如く三層にすれば更に安全性が高くなる。この場合も動作は同様であるが、メモリ１６及び３０に鍵K_xが記憶される点が異なる。この場合、鍵K_tは毎分あるいは毎秒単位で変更され、鍵K_xが週、月或は年単位で変更される。鍵K_tは第１図のＱＰＳＫ復調回路１３の出力中に含まれているので、音声データ信号と共に記録され、音声データ信号と共に再生される。この場合は、第６図Ａの制御情報は鍵K_xで暗号化されており、鍵K_xで復号化して得られた第６図Ｂの制御信号の中に鍵K_t即ち所定のＰＮ初期値が入っている。第５図のデスクランブル処理部３２では、このＰＮ初期値により、映像信号や音声データ信号を復号化（デスクランブル化）する。

発明の効果

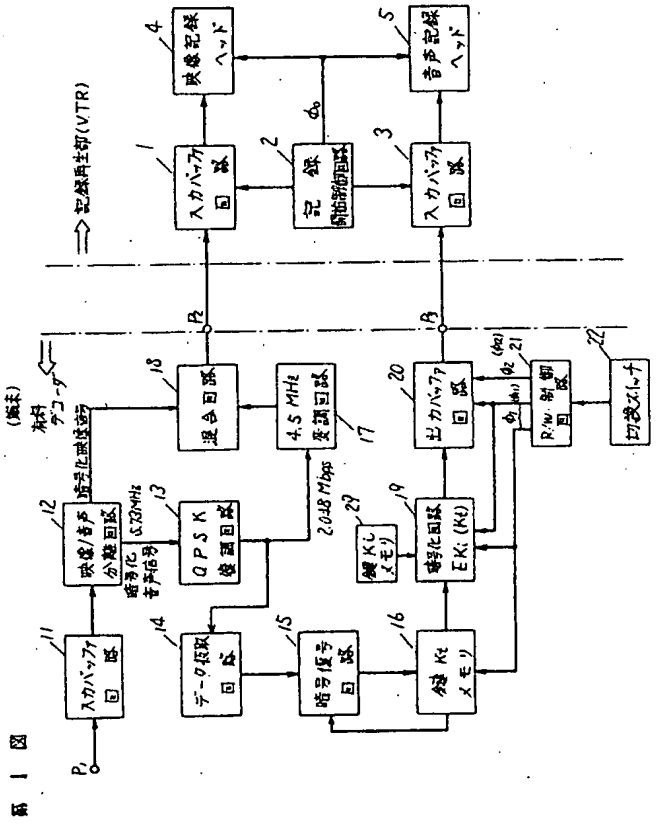
このように、本発明によれば、暗号化した映像信号と、時間の経過により更新される鍵とを、固有の鍵によって暗号化してＶＴＲ等により同一の記録媒体に記録するようにしているので、その記録に用いた固有の鍵を有する暗号解読装置でのみ再生し復号化することができる。従って、不正に記録したＶＴＲテープ等の記録媒体を複写しても、その記録に使用した有料デコーダ等の暗号解読装置を用いない限り、再生して復号化（デスクランブル化）できないので、実質的に不正コピーを防止することができる。

４、図面の簡単な説明

第１図は本発明の一実施例における記録システムの記録部分を示すブロック図、第２図，第３図はその暗号化及び復号化の基本原理を示すブロック図、第４図はその記録タイミングを示すタイミングチャート、第５図は同記録システムの再生部分を示すブロック図、第６図，第７図，第８図は暗号化信号を示す波形図、第９図は本発明の他の実施例における記録システムの要部を示すブロック図である。

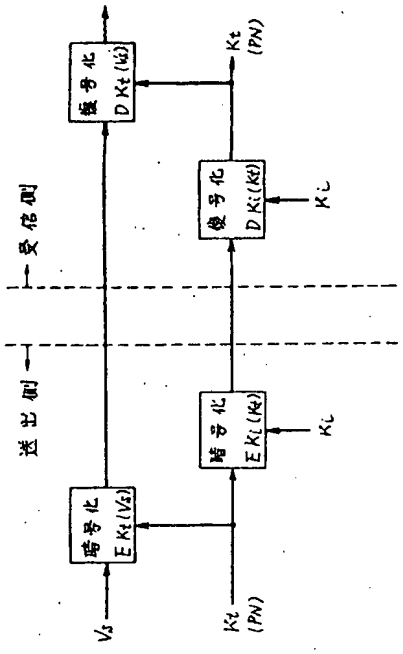
４……映像記録ヘッド、５……音声記録ヘッド、１３……ＱＰＳＫ復調回路、１４……データ抜取回路、１５……暗号復号化回路、１６……K_tメモリＡ、１９……暗号化回路、２５……音声検波回路、２６……セレクタ、２８……復号化回路、２９……K_iメモリ、３０……K_tメモリＢ、３２……デスクランブル処理部。

代理人の氏名　弁理士　栗　野　重　孝　ほか１名

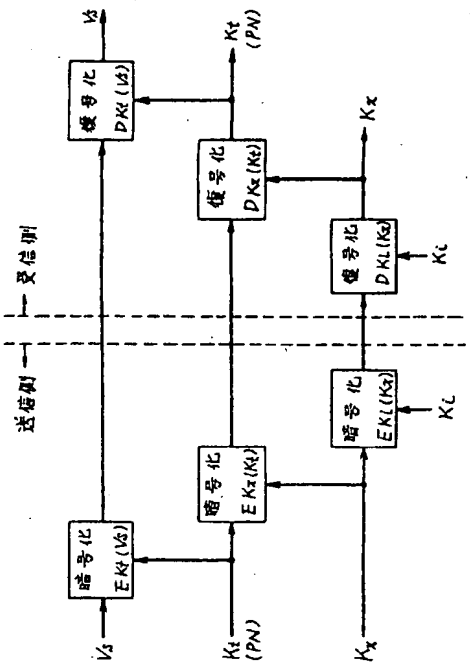


第１図

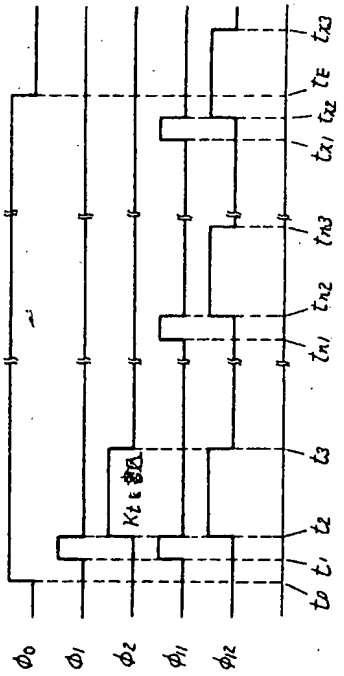
第2図



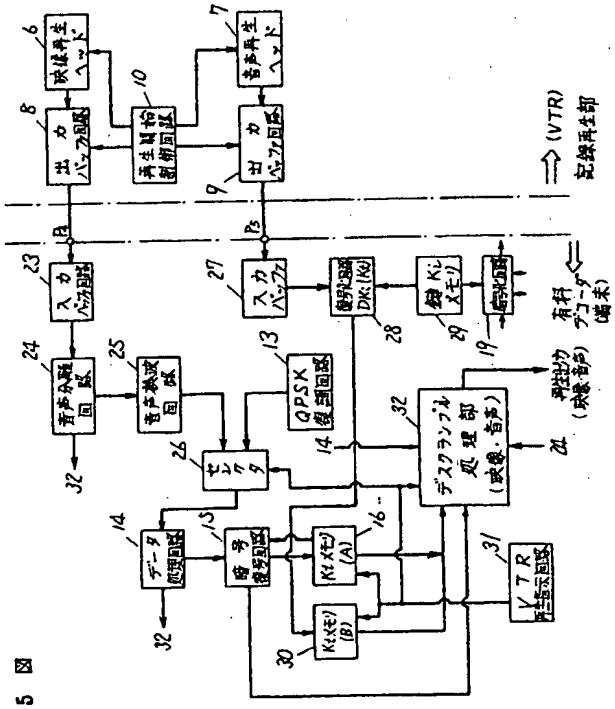
第3図



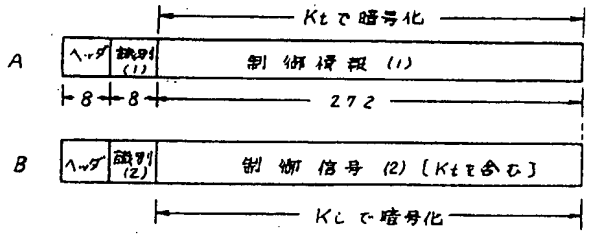
第4図



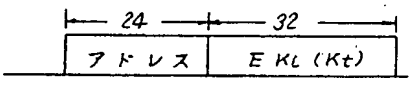
第5図



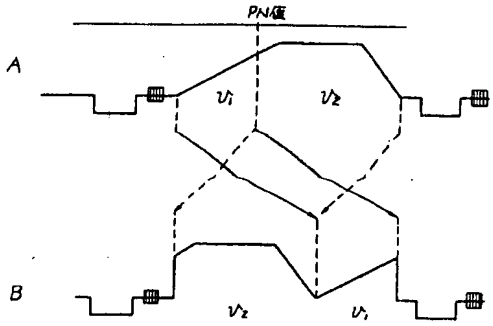
第 6 図



第 7 図



第 8 図



第 9 図